Le 12 décembre 2007 FIN C

2127 **Instruction du Conseil-exécutif concernant la sûreté de l'information et la protection des données (SIPD)**

*Le Conseil-exécutif du canton de Berne,*

au vu de l'article 23, alinéa 1 de la loi sur l'organisation du Conseil-exécutif et de l'administration (LOCA)[1] et de l'article 38 de la loi du 19 février 1986 sur la protection des données (LCPD)[2],

sur proposition de la Direction des finances,

*arrête:*

## 1. Dispositions générales

Champ d'application

**Art. 1** [1] La présente instruction s'applique aux projets et applications du canton dans le domaine des technologies de l'information et de la télécommunication.

[2] Lorsque des indemnités au sens de la loi du 16 septembre 1992 sur les subventions cantonales (LCSu)[3] sont octroyées pour des projets informatiques dont les traitements de données sont soumis à la LCPD, le requérant ou la requérante peut être tenu(e) de se conformer soit aux dispositions matérielles de la présente instruction (art. 4 et instructions spécifiques prévues à l'art. 11), soit aux dispositions d'une norme SIPD établie, reconnue et équivalente. Cette condition est imposée en règle générale lorsque l'existence d'exigences SIPD poussées (art. 4, al. 3) est prévisible.

Responsabilités

**Art. 2** [1] Sont responsables de la SIPD les services qui, dans l'accomplissement de leurs tâches légales, traitent des données, en

[1] RSB 152.01
[2] RSB 152.04
[3] RSB 641.1

particulier des données personnelles, ou en confient le traitement à des tiers (services responsables).

[2] Lorsque plusieurs services traitent conjointement des données, il convient de définir par écrit lequel d'entre eux assume la responsabilité principale de la SIPD.

Obligations du service responsable

**Art. 3** Le service responsable veille à ce que toutes les applications informatiques avec lesquelles sont traitées des données personnelles soient conformes aux prescriptions légales ou contractuelles déterminantes en matière de protection des données et à ce que la sûreté de l'information soit garantie de manière appropriée dans le traitement des données.

## 2. SIPD dans le déroulement des projets informatiques

Analyse SIPD et concept SIPD

**Art. 4** [1] Le comité de projet de chaque projet informatique désigne un ou une responsable SIPD dans le cadre de l'organisation du projet.

[2] Le service responsable réalise une analyse SIPD durant la phase de d'analyse préliminaire pour évaluer la conformité du projet à la législation de la protection des données et détermine à l'aide d'une classification si le projet informatique présente des exigences poussées en matière de SIPD.

[3] Les exigences SIPD sont poussées, en particulier, lorsque

*a* la valeur de remplacement de l'infrastructure (matériel et système d'exploitation) est élevée,

*b* une défaillance des systèmes informatiques pendant plus d'un jour ouvré aurait des conséquences graves pour l'accomplissement des tâches,

*c* la restauration des données impliquerait des problèmes majeurs,

*d* les données traitées sont soumises à des prescriptions légales ou contractuelles concernant le maintien du secret (p. ex. secret professionnel),

*e* une violation de la protection des données aurait des conséquences très dommageables pour les intéressés, ce qui est généralement le cas lors du traitement de données particulièrement dignes de protection.

[4] S'il ressort de l'analyse SIPD qu'il n'existe pas d'exigences SIPD poussées, le service responsable s'assure, lors de la mise en service de l'application informatique, que les prescriptions déterminantes en matière de protection des données sont respectées et que la sûreté de l'information est garantie au minimum par la mise en œuvre des mesures de protection de base SIPD.

[5] Si l'analyse met en lumière des exigences SIPD poussées, il convient d'élaborer un concept SIPD au plus tard durant la phase de conception. Ce concept doit définir, à partir d'une analyse de risques, les mesures organisationnelles et techniques qui sont nécessaires pour procurer une sûreté appropriée de l'information et une protection adéquate des données, et créer les conditions pour que ces mesures soient mi-

ses en œuvre dès la mise en service de l'application informatique.

Documents requis pour l'autorisation des projets informatiques et des moyens financiers correspondants

**Art. 5** [1] Les demandes d'autorisation de crédit contiennent les documents SIPD élaborés.

[2] Si le projet présente des exigences SIPD poussées, les demandes d'autorisation contiennent aussi une prise de position du Bureau pour la surveillance de la protection des données, qui évalue si la LCPD et les autres dispositions SIPD sont respectées. Les documents sont remis en même temps au DSI BE (art. 9).

[3] Le Bureau pour la surveillance de la protection des données doit élaborer sa prise de position dans un délai maximal de trois semaines. Il peut aussi le faire, le cas échéant, pendant la procédure de corapport.

[4] Lorsque des indemnités sont octroyées en faveur de projets assortis de conditions SIPD pour lesquels une autre norme SIPD a été choisie (art. 1, al. 2), les documents requis selon cette norme sont fournis à la place de l'analyse et du concept SIPD. Dans ce cas, les alinéas 2 et 3 s'appliquent indépendamment du fait que le projet présente ou non des exigences SIPD poussées. Les documents définissant la norme SIPD choisie doivent aussi être fournis immédiatement sur demande.

Conséquences du non-respect de la présente instruction

**Art. 6** [1] En cas d'omission de l'analyse SIPD ou d'un concept SIPD actuel, ou s'il s'avère à l'examen que le projet informatique n'est pas conforme aux prescriptions en matière de protection des données ou qu'il ne garantit pas la sûreté de l'information, le mandant refuse de donner son feu vert pour la phase ultérieure du projet et la mise en service n'est pas autorisée.

[2] La sûreté de l'information n'est pas garantie, en particulier, lorsque la mise en service de l'application informatique présente encore des risques jugés élevés en matière de sécurité.

## 3. SIPD dans les applications existantes

Analyse SIPD et concept SIPD pour les applications existantes

**Art. 7** [1] Une analyse SIPD doit être réalisée pour toutes les applications existantes dans le domaine des technologies de l'information et de la communication.

[2] Pour les applications informatiques qui présentent un besoin de protection poussée du fait de leur classification, il convient de définir un concept SIPD comprenant notamment une analyse de risques et une planification contraignante des mesures à adopter pour éliminer les risques importants.

Contrôle périodique des applications informatiques

**Art. 8** [1] Le Conseil-exécutif désigne tous les deux ans les applications informatiques qui doivent être soumises à un contrôle SIPD. Il définit l'objet et l'étendue de ce contrôle.

[2] La Direction de la justice, des affaires communales et des affaires ecclésiastiques présente une proposition. Elle se procure au préalable un corapport de la Direction des finances et des Directions concernées. Les obligations de contrôle prévues dans des dispositions spéciales demeurent réservées.

[3] Les services responsables des applications désignées sont tenus de

confier le contrôle à un service spécialisé externe et indépendant.

[4] La Direction de la justice, des affaires communales et des affaires ecclésiastiques veille à ce que les crédits nécessaires soient mis à disposition. A titre de valeur indicative, ils doivent représenter un pour mille des coûts d'exploitation budgétés pour les moyens informatiques de l'administration cantonale.

## 4. Surveillance et dispositions d'exécution

Surveillance

**Art. 9** [1] C'est au Bureau pour la surveillance de la protection des données qu'il incombe de surveiller que les dispositions sur la protection des données sont respectées et que la sûreté de l'information est garantie en ce qui concerne le traitement des données personnelles (art. 34 LCPD).

[2] Il travaille conjointement avec le ou la délégué-e cantonal-e à la sécurité informatique de l'OIO (DSI BE), qui l'assiste dans sa tâche de surveillance.

[3] C'est au DSI BE ou à la DSI BE qu'il incombe de surveiller que la sûreté de l'information est garantie dans les activités qui n'impliquent pas le traitement de données personnelles. Il ou elle peut être invité(e) à coopérer aux projets informatiques en tant que conseiller ou conseillère.

[4] Les services soumis à la présente instruction (art. 1, al. 1) remettent au Bureau pour la surveillance de la protection des données et au DSI BE ou à la DSI BE, pour information, leurs instructions en matière de SIPD une semaine au plus tard avant de les édicter. Le Bureau pour la surveillance de la protection des données et le ou la DSI BE doivent être dûment associés aux projets normatifs en matière de SIPD.

Personnes de contact du Bureau pour la surveillance de la protection des données et du ou de la DSI BE

**Art. 10** [1] Les Directions et la Chancellerie d'Etat désignent un ou une responsable de la sécurité informatique (RSI BE) en tant que principale personne de contact du DSI BE ou de la DSI BE.

[2] Les Directions et la Chancellerie d'Etat désignent un Service de conseil en matière de protection des données dans les projets informatiques (SCPD BE) en tant que principal contact du Bureau pour la surveillance de la protection des données pour les questions relatives aux technologies de l'information et de la télécommunication, à moins que des conseillers ou conseillères à la protection des données au sens du chiffre 1 de l'ACE n° 1102 du 9 avril 2003 « Beratung bei Datenschutzfragen » n'aient déjà été désignés.

Instructions de l'Office d'informatique et d'organisation

**Art. 11** [1] Après avoir consulté les Directions, la Chancellerie d'Etat, le Bureau pour la surveillance de la protection des données et la Conférence informatique cantonale (CIC), l'Office d'informatique et d'organisation (OIO) édicte les instructions d'exécution nécessaires, concernant notamment

*a* l'analyse SIPD et la classification SIPD à réaliser pour les projets informatiques,

*b* le concept SIPD à définir pour les projets informatiques,

*c* la protection de base SIPD à respecter,

*d* les conditions générales SIPD du canton (CG SIPD) qui doivent impérativement être respectées ou prescrites pour les projets informatiques ; elles peuvent prévoir l'intégration dans les contrats des bases SIPD définies (lettres a à c).

[2] L'OIO met à disposition des outils adéquats (explications, listes de contrôle, etc.) et fournit une offre de conseil et de formation appropriée.

## 5. Dispositions finales

Abrogation et adaptation d'arrêtés du Conseil-exécutif

**Art. 12** [1] L'ACE 4637 du 9 décembre 1992 « Mindestanforderungen an die Datensicherheit » est abrogé.

[2] Dans l'ACE 0330 du 24 janvier 2001 « Betriebsbewilligung des Regierungsrats für das Informationssystem der Kantonspolizei gemäss Artikel 52 Absatz 2 PolG » n'existant qu'en allemand, l'alinéa 2 du chiffre 8 est modifié.

[3] L'ACE 1103 du 9 avril 2003 « Datenschutz bei Informatikanwendungen » est abrogé.

[4] L'ACE 1104 du 9 avril 2003 « Datenschutz bei Informatikprojekten » est abrogé.

[5] Dans l'ACE 1668 du 26 mai 2004 « Datenschutz; Periodische Prüfung von Informatikanwendungen; Rahmenbedingungen für den Beizug externer Kontrollstellen », les références à des dispositions en matière de sûreté de l'information et de protection des données qui ne sont plus en vigueur s'entendent comme des références aux dispositions SIPD actuelles.

Entrée en vigueur

**Art. 13** La présente instruction entre en vigueur le 1er janvier 2008.

Aux Directions et
à la Chancellerie d'Etat

Certifié exact

le chancelier :